UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA v. ASHRAF AL SAFOO	Case No. 18 CR 696 Judge John Robert Blakey

PROTECTIVE ORDER PURSUANT TO SECTION 3 OF THE CLASSIFIED INFORMATION PROCEDURES ACT

This matter comes before the Court upon the government's motion for a protective order to prevent the unauthorized use, disclosure or dissemination of classified national security information and documents that will be reviewed by or made available to, or are otherwise in the possession of, defense counsel in this case.

Pursuant to Sections 3 and 9 of the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. 3 (2006), the Security Procedures established pursuant to Section 9(a) of CIPA by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9) (hereinafter the "Security Procedures"); the Federal Rules of Criminal Procedure 16(d) and 57; the general supervisory authority of the Court; and, in order to protect the national security, the following Protective Order Pursuant to Section 3 of CIPA ("Order") is entered.

IT IS HEREBY **ORDERED:**

1. This case involves information classified in the interest of the national security of the United States pursuant to Executive Order 13526, as amended. The storage, handling, and control of this information require special security

precautions, and access to this information requires an appropriate security clearance and a need-to-know determination pursuant to Executive Order 13526, as amended.

2. This Order establishes the procedures that must be followed by all defense counsel of record, their designated employees, all other counsel involved in this case, translators for the defense, any Court personnel, and all other individuals who receive access to classified information or documents in connection with this case. These procedures will apply to all pretrial, trial, post-trial and appellate matters concerning classified information in this case and may be modified from time to time by further order of the Court pursuant to Sections 3 and 9 of CIPA, Rule 16(d) of the Federal Rules of Criminal Procedure, and the Court's inherent supervisory authority to ensure fair and expeditious proceedings.

Definitions

3. As used herein, the terms "classified national security information and documents," "classified information," "classified documents," and "classified material" refer to:

A. Any document or information that has been classified by any Executive Branch agency in the interest of national security or pursuant to Executive Order 13526, as amended, or its predecessor orders, as "CONFIDENTIAL," "SECRET," or "TOP SECRET," or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION" ("SCI"), or any information contained in such documents;

B. Any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party, which has been derived from a United States Government classified document, information, or material, regardless of whether such document, information, or material has itself subsequently been classified by the Government pursuant to Executive Order 13526, as amended, or its predecessor orders, as "CONFIDENTIAL," "SECRET," or "TOP SECRET," or additionally controlled as "SCI";

C. Classified information conveyed verbally to defense counsel, the Defendant, or any employee of defense counsel;

D. Any document or information, including verbal information, which defense counsel have been notified orally or in writing contains classified information; and

E. "Foreign government information" as that term is defined in Executive Order 13526, as amended, or its predecessor orders.

4. The words "documents," "information," and "material" shall include but are not limited to all written or printed matter of any kind, formal or informal, including originals, conforming copies and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), and further include but are not limited to:

A. Papers, correspondence, memoranda, notes, letters, reports, summaries, photographs, maps, charts and graphs, interoffice and intra-office communications, notations of any sort concerning conversations, meetings or other

communications, bulletins, teletypes, telegrams and telefacsimiles, invoices, worksheets and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

B. Graphic or oral records or representations of any kind, including but not limited to photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;

C. Electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and

D. Information acquired orally or verbally.

5. "Access to classified information" means having access to, reviewing, reading, learning or otherwise coming to know in any manner any classified information.

6. "Secure Area" shall mean a physical facility approved by the Classified Information Security Officer for the storage, handling, and control of classified information at a level appropriate for the classification of the information.

7. All classified documents or material and the information contained therein shall remain classified unless the documents or material bear a clear indication that they have been declassified by the agency or department that is the originating agency (hereinafter the "Originating Agency") of the document, material, or information contained therein.

8. Classified Information Security Officer. In accordance with the provisions of CIPA and the Security Procedures, the Court has designated Daniel O. Hartenstine as Classified Information Security Officer ("CISO") for this case, and Debra M. Guerrero-Randall, Joan B. Kennedy, Shawn P. Mahoney, Maura L. Peterson, Carli V. Rodriguez-Feo, Harry J. Rucker, and W. Scooter Slade as Alternate Classified Information Security Officers for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information to be made available in connection with this case. Defense counsel shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

9. Government Attorneys. The Court has been advised that the Government attorneys working on this case, Barry Jonas, Vikas Didwania, Melody Wells and Peter Salib, and their respective supervisors (collectively referred to hereinafter as the "Government Attorneys"), have the requisite security clearances to have access to the classified information that relates to this case.

10. Protection of Classified Information. The Court finds that, in order to protect the classified information involved in this case, only appropriately cleared Government Attorneys, Department of Justice employees, personnel of the Originating Agency, defense counsel, employees of defense counsel, or translators employed by defense counsel, shall have access to the classified information in this case.

A. Defense counsel, employees of defense counsel or defense translators may obtain access to classified documents or information only if such person has:

1. Received the necessary security clearance at the appropriate level of classification, through or confirmed by the CISO;

2. Received permission of the Court, either through this Order (for those named in paragraph 11 below) or by a separate Court order upon showing of a need-to-know; and

3. Signed the Memorandum of Understanding in the form attached hereto, agreeing to comply with the terms of this Order.

B. Before receipt of any classified information, defense counsel shall file originals of the executed Memoranda of Understanding with the Court and the CISO and serve copies of such document upon the Government.

C. The substitution, departure and removal for any reason from this case of counsel for the defendant, or anyone associated with the defense as an employee or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

11. Defense Counsel. Subject to the provisions of paragraph 10, the following attorney(s) for the defense and their approved employee(s) and translator(s) (collectively referred to hereinafter as "the Defense"), may be given access to classified information as required by the Government's discovery obligations: Thomas A. Durkin and Joshua G. Herman. Any additional person whose assistance the Defense

reasonably requires may have access to classified information in this case only after obtaining from the Court – with sufficient prior notice to the Government – an approval for access to the appropriate level of classification on a need-to-know basis, and after satisfying the other requirements described in this Order for access to classified information.

12. The fact that one person holds an appropriate security clearance and is approved for access to classified documents or information does not give that person the authority to disclose any classified documents or information to any other individual. By way of example, but not limitation, defense counsel are not authorized to discuss or otherwise disclose classified documents or information with the defendant absent written permission of the Government. To the extent the defendant may, pursuant to and in the course of the Government's discovery obligations, be allowed to review any classified documents or information, an appropriate separate order may be entered regarding those items.

13. Secure Area of Review. The CISO, in consultation with the Court and U.S. Marshal, shall arrange for an approved Secure Area for use by the Defense. The CISO shall establish procedures to assure that the Secure Area is accessible for the Defense during normal business hours, and by exception, after hours or on weekends upon request of the CISO and in consultation with the Court and U.S. Marshals Service. The Secure Area shall contain a separate working area for the Defense and will be outfitted with any secure office equipment requested by the Defense that is reasonable and necessary to the preparation of the defense in this case. The CISO, in

consultation with defense counsel, shall establish procedures to assure that the Secure Area may be maintained and operated in the most efficient manner consistent with the protection of classified information at the level necessary based on its level of classification. No documents or other material containing classified information may be removed from the Secure Area unless authorized by the CISO. The secure area shall not be accessible to the Government Attorneys. The CISO shall not reveal to the Government the content of any conversations he or she may hear among the Defense, nor reveal the nature of documents being reviewed by them, nor the work generated by them. In addition, the presence of the CISO shall not operate to waive, limit, or otherwise render inapplicable, the attorney-client privilege.

14. Filings with the Court. Until further order of this Court, any motion, memorandum, or other document filed by the Defense that defense counsel knows, or has reason to believe, contains classified information in whole or in part, or any document the proper classification of which defense counsel is unsure, shall be filed under seal with the Court through the CISO or an appropriately cleared designee of his choosing. Pleadings filed under seal with the CISO shall be marked "Filed In Camera and Under Seal with the Classified Information Security Officer" and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the CISO or a designee shall be considered as the date and time of court filing. At the time of making a physical submission to the CISO or a designee, counsel shall file on the public record in the

CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title of the filing. The CISO shall make arrangements for prompt delivery under seal to the Court and counsel for the Government any document to be filed by the Defense that contains classified information. The CISO shall promptly examine the document and, in consultation with representatives of the appropriate Government agencies, determine whether the document contains classified information. If the CISO determines that the document contains classified information, he or she shall ensure that the classified portions of the document, and only those portions, are marked with the appropriate classification marking and that the document remains under seal. All portions of any document filed by the Defense that do not contain classified information shall immediately be unsealed by the CISO and placed in the public record.

15. Any document filed by the Government containing classified information shall be filed under seal with the Court through the CISO or an appropriately cleared designee of his choosing. Pleadings filed under seal with the CISO or a designee shall be marked "Filed In Camera and Under Seal with the Classified Information Security Officer" and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the CISO or a designee, which should occur no later than 4:00 p.m., shall be considered the date and time of filing. Unless the pleading is filed "Ex Parte," the CISO shall make arrangements for prompt delivery under seal to the

Court and defense counsel in a secure area any document to be filed by the Government that contains classified information. At the time of making a physical submission to the CISO or a designee, counsel shall file on the public record in the CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title of the filing.

16. Sealing of Records: The CISO shall maintain a separate sealed record for those pleadings containing classified materials and retain such record for purposes of later proceedings or appeal.

17. Access to Classified Information. Defense counsel and designated employees shall have access to classified information only as follows:

A. All classified information produced by the Government to the Defense, in discovery or otherwise, and all classified information possessed, created or maintained by the Defense, shall be stored, maintained and used only in the Secure Area established by the CISO;

B. The Defense shall have free access to the classified information made available to them in the Secure Area and shall be allowed to take notes and prepare documents with respect to those materials. However, the Defense shall not, except under separate Court order, disclose the classified information, either directly, indirectly, or in any other manner which would disclose the existence of such, to pursue leads or in the defense of the defendant;

C. The Defense shall not copy or reproduce any classified information in any form, except with the approval of the CISO, or in accordance with the procedures established by the CISO for the operation of the Secure Area;

D. All documents prepared by the Defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information, shall be transcribed, recorded, typed, duplicated, copied or otherwise prepared only by persons who have received an appropriate approval for access to classified information, and in the Secure Area on equipment approved for the processing of classified information, and in accordance with the procedures established approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, etc.) containing classified information shall be maintained in the Secure Area, unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the Government;

E. The Defense shall discuss classified information only within the Secure Area or in another area authorized by the CISO, and shall not discuss or attempt to discuss classified information over any standard commercial telephone instrument or office intercommunication system; and

F. The Defense shall not disclose, without prior approval of the Court, any classified information to any person not authorized pursuant to this Order, including the defendant and defense witnesses, except the Court, appropriately

cleared court personnel, and the Government Attorneys who have been identified by the CISO as having the appropriate clearances and the need-to-know that information. Any person approved by the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to the Court, under seal, the Memorandum of Understanding appended to this Order, and to comply with all terms and conditions of this Order. If preparation of the Defense requires that classified information be disclosed to persons not named in this Order, then, upon approval by the Court and upon prior notice to the Government, the CISO shall promptly seek to obtain security clearances for them at the request of defense counsel.

18. Foreign Intelligence Surveillance Act (FISA). The defendant has rights under the United States Constitution, federal statutes, and the Federal Rules of Criminal Procedure to pre-trial discovery. The Government recognizes its obligation to provide such discovery materials to defense counsel in the most expeditious manner possible, consistent with public safety and the confidentiality of sensitive ongoing investigations. Therefore, to the extent that FISA-obtained or derived information is provided to the defense counsel:

A. Both the Defense and the Government shall have access to such FISA information regardless of prior minimization efforts undertaken by the Government upon initial review. It is contemplated that the Government may produce material to the Defense determined to be relevant to the proceedings even if not deemed pertinent when the material was initially reviewed;

B. Any draft transcripts or summaries of translated electronic and paper materials that may be provided shall not be used in any proceeding for any purpose, including cross-examination of any witness, except pursuant to further order of this Court; and

C. Notwithstanding any other provisions of this Order or any subsequent order, the disclosure and discovery of materials that may be provided to the Court, *in camera* and *ex-parte*, pursuant to FISA for legal determinations, including but not limited to any FISA applications, orders, or materials, shall be governed by the provisions of FISA.

19. Procedures for the use or disclosure of classified information by the Defense shall be those provided in Sections 5, 6 and 8 of CIPA. To facilitate the Defense's filing of notices required under Section 5 of CIPA, the CISO shall make arrangements with the appropriate agencies for a determination of the classification level, if any, of materials or information, either within the possession of the Defense or about which the Defense has knowledge and intends to use in any way at any pre-trial proceeding, deposition or at trial. Nothing submitted by the Defense to the CISO pursuant to this paragraph shall be made available to the Government Attorneys unless so ordered by the Court, or so designated by the Defense. Should the CISO confirm that the material or information is classified and the Defense intends to use such classified information, the Defense shall file a CIPA Section 5 notice. The Defense shall not use, disclose or cause to be disclosed any classified information in any manner in connection with any trial or pre-trial proceeding contrary to this Order

or other order of this Court, unless and until the procedures under CIPA have been followed or waived by the Government in writing.

20. Violations of this Order. Unauthorized use or disclosure of classified information may constitute violations of United States criminal laws. In addition, violation of the terms of this Order shall be immediately brought to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order will result in the termination of a person's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized use, disclosure, retention or negligent handling of classified information could cause serious damage to the national security of the United States or may be used to the advantage of a foreign nation against the interests of the United States. This Order is to ensure that those authorized by the Order to receive classified information will never divulge the classified information disclosed to them to anyone who is not authorized to receive it, or otherwise use the classified information, without prior written authorization from the Originating Agency and in conformity with this Order.

21. All classified information to which the Defense has access in this case is now and will remain the property of the United States Government. The defense counsel, defense counsel employees, defense translators, and anyone else who receives classified information pursuant to this Order shall return all such classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information,

to the CISO upon request. The notes, summaries and other documents prepared by the Defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of this case. At the conclusion of all proceedings, including any final appeals, all such notes, summaries and other documents are to be destroyed by the CISO in the presence of defense counsel if so desired.

22. Declassified Information. As used herein, the term "declassified information" refers to any and all classified information, which may be declassified pursuant to the appropriate procedures of the original classifying authority. Any declassified information will be treated by the defense as "Sensitive Discovery Materials" under the Protective Order titled *Protective Order General and Sensitive Discovery Material*.

23. Nothing in this Order shall preclude the Government from seeking further protective orders pursuant to CIPA, FISA, and/or Rule 16(d) as to particular items of discovery material.

24. A copy of this Order shall be issued forthwith to counsel for the defendant, who shall be responsible for advising the defendant and defense counsel employees, of the contents of this Order.

Dated: April 10, 2019

Entered:

John Robert Blakey
United States District Judge